

10 / 531173

11 APR 2005

PCT/JP2004/000709

27.1.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

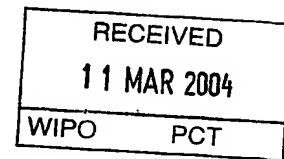
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2003年 1月29日

出 願 番 号
Application Number: 特願2003-021039
[ST. 10/C]: [JP2003-021039]

出 願 人
Applicant(s): キヤノン株式会社

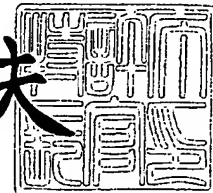


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 2月26日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2004-3013748

BEST AVAILABLE COPY

【書類名】 特許願
【整理番号】 251538
【提出日】 平成15年 1月29日
【あて先】 特許庁長官殿
【国際特許分類】 B41K 3/00
【発明の名称】 認証装置
【請求項の数】 19
【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

【氏名】 鳥居 寛

【特許出願人】

【識別番号】 000001007

【氏名又は名称】 キヤノン株式会社

【代理人】

【識別番号】 100076428

【弁理士】

【氏名又は名称】 大塚 康德

【電話番号】 03-5276-3241

【選任した代理人】

【識別番号】 100112508

【弁理士】

【氏名又は名称】 高柳 司郎

【電話番号】 03-5276-3241

【選任した代理人】

【識別番号】 100115071

【弁理士】

【氏名又は名称】 大塚 康弘

【電話番号】 03-5276-3241

【選任した代理人】

【識別番号】 100116894

【弁理士】

【氏名又は名称】 木村 秀二

【電話番号】 03-5276-3241

【手数料の表示】

【予納台帳番号】 003458

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0102485

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証装置

【特許請求の範囲】

【請求項 1】 複数の認証機構を備える認証装置であって、
ユーザの認証情報を入力する入力手段と、
前記入力手段により入力された前記認証情報が前記複数の認証機構を切換え可能なユーザのものかどうかを判定する判定手段と、
前記判定手段により前記切換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御手段と、
前記表示制御手段により表示された前記一覧の中の選択された認証機構を有効な認証機構として登録する登録手段と、
を有することを特徴とする認証装置。

【請求項 2】 複数の認証機構を備える認証装置であって、
ユーザの認証情報を入力する入力手段と、
前記入力手段により入力された前記認証情報が前記複数の認証機構を切換え可能なユーザのものかどうかを判定する判定手段と、
前記判定手段により前記切換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御手段と、
前記表示制御手段により表示された前記一覧の中の認証機構を選択する選択手段と、
前記選択手段により選択された認証機構が前記入力手段により入力された認証情報を登録している場合に、前記選択手段により選択された前記認証機構を有効な認証機構として登録する登録手段と、
を有することを特徴とする認証装置。

【請求項 3】 前記入力手段は、ユーザの認証情報を記録したカードを読み取って前記認証情報を入力することを特徴とする請求項 1 又は 2 に記載の認証装置。

【請求項 4】 前記入力手段は、ウェブブラウザにより前記認証情報を入力することを特徴とする請求項 1 又は 2 に記載の認証装置。

【請求項 5】 前記複数の認証機構のそれぞれは、
ユーザの認証情報を登録している記憶手段と、
入力されたユーザの認証情報が前記記憶手段に登録されている場合に、当該ユーザを認証する認証判定手段と、
を有することを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の認証装置。

【請求項 6】 前記登録手段により有効な認証機構として登録されている認証機構を起動する起動手段を更に有することを特徴とする請求項 1 乃至 5 のいずれか 1 項に記載の認証装置。

【請求項 7】 複数の認証機構を備える認証装置における認証方法であって、
ユーザの認証情報を入力する入力工程と、
前記入力工程で入力された前記認証情報が前記複数の認証機構を切り換え可能なユーザのものかどうかを判定する判定工程と、
前記判定工程で前記切り換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御工程と、
前記表示制御工程で表示された前記一覧の中の選択された認証機構を有効な認証機構として登録する登録工程と、
を有することを特徴とする認証方法。

【請求項 8】 複数の認証機構を備える認証装置における認証方法であって、
ユーザの認証情報を入力する入力工程と、
前記入力工程で入力された前記認証情報が前記複数の認証機構を切り換え可能なユーザのものかどうかを判定する判定工程と、
前記判定工程で前記切り換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御工程と、
前記表示制御工程で表示された前記一覧の中の認証機構を選択する選択工程と、
前記選択工程で選択された認証機構が、前記入力工程で入力された認証情報を登録している場合に前記選択工程で選択された前記認証機構を有効な認証機構と

して登録する登録工程と、
を有することを特徴とする認証方法。

【請求項 9】 前記入力工程では、ユーザの認証情報を記録したカードを読み取って前記認証情報を入力することを特徴とする請求項 7 又は 8 に記載の認証方法。

【請求項 10】 前記入力工程では、ウェブブラウザにより前記認証情報を入力することを特徴とする請求項 7 又は 8 に記載の認証方法。

【請求項 11】 前記複数の認証機構のそれぞれは、ユーザの認証情報を登録する記憶ユニットを有し、入力されたユーザの認証情報が前記記憶ユニットに登録されている場合に、当該ユーザを認証する認証判定工程と、
を有することを特徴とする請求項 7 乃至 10 のいずれか 1 項に記載の認証方法。

【請求項 12】 前記登録工程で有効な認証機構として登録されている認証機構を起動する起動工程を更に有することを特徴とする請求項 7 乃至 11 のいずれか 1 項に記載の認証方法。

【請求項 13】 ユーザ認証情報を入力する入力工程と、
前記入力工程において入力されたユーザの認証情報を用いて第 1 システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第 1 システムに加入させる第 1 認証工程と、

前記入力工程において入力されたユーザの認証情報を用いて第 2 システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第 2 システムに加入させる第 2 認証工程と、

前記ユーザを、前記第 1 システムの管理下で管理するのか、又は、前記第 2 システムの管理下で管理するのかを制御する制御工程と、

前記第 2 認証工程において前記ユーザの前記第 2 システムに対する認証が成功したことを確認する確認工程と、

前記第 1 システムから前記第 2 システムの管理下へユーザを移行させる命令を認識した場合には、前記制御工程は、前記確認工程において、前記ユーザが前記第 2 認証工程にて認証されたことを確認したことを条件として、前記第 1 システムにおける管理下から前記第 2 システムにおける管理下に前記ユーザを移行させ

るべく前記第1認証工程及び前記第2認証工程を制御することを特徴とする認証方法。

【請求項14】 前記制御工程は、前記確認工程において、前記ユーザが前記第2認証工程にて認証されたことが確認された場合に、前記ユーザを前記第1認証工程の管理対象外となるよう前記第1認証工程を制御することを特徴とする請求項13に記載の認証方法。

【請求項15】 前記第1認証工程は、ユーザレベルのアクセス権限を認証するものであり、前記第2認証工程は管理者レベルのアクセス権限を管理するものであることを特徴とする請求項13又は14に記載の認証方法。

【請求項16】 ユーザ認証情報を入力する入力手段と、

前記入力手段により入力されたユーザの認証情報を用いて第1システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第1システムに加入させる第1認証手段と、

前記入力手段により入力されたユーザの認証情報を用いて第2システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第2システムに加入させる第2認証手段と、

前記ユーザを、前記第1システムの管理下で管理するのか、又は、前記第2システムの管理下で管理するのかを制御する制御手段と、

前記第2認証手段により前記ユーザの前記第2システムに対する認証が成功したことを確認する確認手段と、

前記第1システムから前記第2システムの管理下へユーザを移行させる命令を認識した場合には、前記制御手段は、前記確認手段において、前記ユーザが前記第2認証手段により認証されたことを確認したことを条件として、前記第1システムにおける管理下から前記第2システムにおける管理下に前記ユーザを移行させるべく前記第1及び第2認証手段を制御することを特徴とする認証装置。

【請求項17】 前記制御手段は、前記確認手段により前記ユーザが前記第2認証手段により認証されたことが確認された場合に、前記ユーザを前記第1認証手段の管理対象外となるよう前記第1認証手段を制御することを特徴とする請求項16に記載の認証装置。

【請求項 18】 前記第 1 認証手段は、ユーザレベルのアクセス権限を認証するものであり、前記第 2 認証手段は管理者レベルのアクセス権限を管理するものであることを特徴とする請求項 16 又は 17 に記載の認証装置。

【請求項 19】 ユーザ認証情報を入力するための入力工程と、

前記入力工程において入力されたユーザの認証情報を用いて第 1 システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第 1 システムに加入させる第 1 認証工程と、

前記入力工程において入力されたユーザの認証情報を用いて第 2 システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第 2 システムに加入させる第 2 認証工程と、

前記ユーザを、前記第 1 システムの管理下で管理するのか、又は、前記第 2 システムの管理下で管理するのかを制御する制御工程と、

前記第 2 認証工程において前記ユーザの前記第 2 システムに対する認証が成功したことを確認する確認工程と、

前記第 1 システムから前記第 2 システムの管理下へユーザを移行させる命令を認識した場合には、前記制御工程は、前記確認工程において、前記ユーザが前記第 2 認証工程にて認証されたことを確認したことを条件として、前記第 1 システムにおける管理下から前記第 2 システムにおける管理下に前記ユーザを移行させるべく前記第 1 認証工程及び前記第 2 認証工程を制御することを特徴とする認証プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数の認証機構を備え、これら複数の認証機構の中から 1 つを有効にしてユーザを認証する技術に関するものである。

【0002】

【従来の技術】

従来、ユーザが所定のユーザであるかどうかを認証し、その認証されたユーザのみがアクセスできるようにしてデータのセキュリティを高めた装置が知られて

いる。このような装置には、ユーザの認証を行う認証機構を単一だけでなく複数備えたものがある。このような複数の認証機構には、それら認証機構を階層的に配置していて、ユーザが上位の認証機構を利用する前に、より下位の認証機構により認証されるようにしたもの、或いは複数の認証機構を並列に配置し、ユーザの認証なく、それら複数の認証機構のいずれかを選択できるようにし、その選択された認証機構を用いてユーザの認証を行うものがある。

【0003】

【発明が解決しようとする課題】

しかしながら、このような従来の技術では、それぞれ利便性とセキュリティの上で問題があった。例えば、認証機構を階層的に配置しているものは、各階層の認証機構を起動する度に、そのユーザの認証情報を提供する必要があり操作が煩わしかった。また認証機構を並列に配置しているものは、ユーザの認証なしに認証機構を切り替えられるため、操作の点では容易であるが、その分セキュリティの面で信頼性が低いという問題があった。

【0004】

本発明は上記従来例に鑑みてなされたもので、利便性とセキュリティ上の問題を解決するために、認証機構の切り替え機能を利用するときに認証情報の提供を促すようにしたものである。

【0005】

また本発明の目的は、認証機構を切り替えた後にユーザが適切な認証情報を持ち合わせていないがために装置を使用することができなくなることを避けるために、認証機構の切り替え前に新しい認証機構によって認証を確認することにある。

【0006】

【課題を解決するための手段】

上記目的を達成するために本発明の認証装置は以下のような構成を備える。即ち、

複数の認証機構を備える認証装置であって、
ユーザの認証情報を入力する入力手段と、

前記入力手段により入力された前記認証情報が前記複数の認証機構を切換え可能なユーザのものかどうかを判定する判定手段と、

前記判定手段により前記切換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御手段と、

前記表示制御手段により表示された前記一覧の中の選択された認証機構を有効な認証機構として登録する登録手段とを有することを特徴とする。

【0007】

また上記目的を達成するために本発明の認証方法は以下のような工程を備える。即ち、

ユーザ認証情報を入力する入力工程と、

前記入力工程において入力されたユーザの認証情報を用いて第1システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第1システムに加入させる第1認証工程と、

前記入力工程において入力されたユーザの認証情報を用いて第2システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第2システムに加入させる第2認証工程と、

前記ユーザを、前記第1システムの管理下で管理するのか、又は、前記第2システムの管理下で管理するのかを制御する制御工程と、

前記第2認証工程において前記ユーザの前記第2システムに対する認証が成功したことを確認する確認工程と、

前記第1システムから前記第2システムの管理下へユーザを移行させる命令を認識した場合には、前記制御工程は、前記確認工程において、前記ユーザが前記第2認証工程にて認証されたことを確認したことを条件として、前記第1システムにおける管理下から前記第2システムにおける管理下に前記ユーザを移行させるべく前記第1認証工程及び前記第2認証工程を制御することを特徴とする。

【0008】

【発明の実施の形態】

以下、添付図面を参照して本発明の好適な実施の形態を詳細に説明する。尚、本実施の形態では、複数の認証機構を搭載したデータ処理装置の場合で、カード

により認証情報の提供を行う場合で説明するが、本発明はこのような構成に限定されるものではない。

【0009】

〔実施の形態1〕

図1は、本発明の実施の形態に係るデータ処理装置の構成を示すブロック図である。

【0010】

図において、100はCPU（中央演算装置）で、本実施の形態で説明する制御方法を実行するプログラムに従って後述する処理を実行する。101はプログラムメモリで、CPU100により実行される制御プログラムが保存されている。102はRAMで、CPU100による制御動作の実行時に、各種データを一時的に記憶するためのメモリエリア（ワークエリア）を提供している。103は表示部で、ユーザへのメッセージやメニュー、及びこの実施の形態では認証機構の一覧等を表示するのに使用される。104はカードリーダーで、ユーザにより提示されるカードを読み取って、そのカードに記憶されている情報を読み取る。105は操作パネルで、キーボードやポインティングデバイス等の入力ユニットを備えており、後述する認証機構の選択等に用いられる。110はこれら各部とCPU100とを接続しているシステムバスで、データバスや制御信号バス等を含んでいる。

【0011】

尚、これ以外にも、プログラムや画像データなどを記憶している大容量の二次記憶装置（ハードディスク或いはMO）、処理結果などを印刷出力するプリンタ等を備えていても良い。

【0012】

図2は、本実施の形態1に係るデータ処理装置の機能構成を示す機能ブロック図である。尚、この実施の形態1では、これら各機能部は、CPU100がプログラムを実行することにより実現されている。

【0013】

図2において、201は認証切り替え部で、管理者名を登録している管理者デ

データベース202を管理するとともに、現在有効な認証機構を記憶している。管理者データベース202は、管理者の名前などの情報を保存している。203は認証機構起動部で、認証機構切り替え部201で指示された認証機構を選択して起動することができる。204と205は、この装置に搭載されている複数の認証機構の内2つを示し、それぞれ第1システムを管理する認証機構Aと第2システムを管理する認証機構Bで表わされている。206, 207は、ユーザの名前などの情報を保存している認証機構データベースであり、それぞれ認証機構A(204)用のものと、認証機構B(205)用のものを備えている。208はユーザインターフェース制御部で、操作パネル105よりの入力及び表示部103への表示を制御して、ユーザへのメッセージや警告などを表示している。カードリーダー104は、ユーザによりカード209を挿入されると、そのカード209に記録されているユーザの名前などの情報を読み取ることができる。この読み取ったカード情報はカードリーダー104から、その時点で起動されている認証機構(204或いは205)に送られる。これにより、その認証機能は対応する認証機構データベースを検索して、そのカードのユーザが、その認証機構のユーザとして登録されているかどうかを判定し、登録されている場合にそのユーザが認証される。このカード209はユーザが持ち歩いているものである。210は管理者、211は一般ユーザである。ここで、システムとは別個に設けられた独立したシステムも含むが、一つのシステムに複数の認証レベルに対応して認証機構が存在した場合も考えられる。例えば、第1認証レベルであるユーザレベルに対応するシステムを第1システム、第2認証レベルである管理者レベルに対応する第2認証レベルに対応するシステムを第2システムと呼ぶことにする。

【0014】

図3は、本実施の形態に係るデータ処理装置における図2の各機能部間でのやりとりを説明する図である。

【0015】

このデータ処理装置の起動時には、まず認証機構起動部203に制御が渡される。この認証機構起動部203は、認証機構切り替え部201に対して、有効な認証機構を問い合わせる(300)。そして、その問合せに対する回答301に

より、認証機構 A (204) 或いは認証機構 B (205) が指示されると、認証機構起動部 203 はその指示された認証機構を起動する (302)。この図 3 では、認証機構 A (204) が有効となっており、この認証機構 A (204) が起動される場合を想定している。こうして起動された認証機構 A (204) は、ユーザインターフェース制御部 208 に対して、ユーザに対してカードリーダー 104 にカードを挿入するように指示するカード挿入指示画面を表示部 103 に表示するよう要求する (303)。この指示要求を受けたユーザインターフェース制御部 208 は、その要求に従ってカードの挿入を促す画面を表示部 103 に表示する。尚、ここで、カードリーダー 104 に挿入するように要求されるカードは、一般ユーザ 211 が所有している認証機構の切り替えを許されていないカードであるとする。

【0016】

こうして、ユーザ 211 のカードがカードリーダー 104 に挿入されると (304)、カードリーダー制御部 220 は、そのカードから読み取った認証情報を認証機構 A (204) に渡す (305)。これにより認証機構 A (204) は、その認証情報を基にして認証機構 A の認証機構データベース 206 に対して検索をかけて (306)、そのユーザの認証情報が認証機構 A (204) のデータベース 206 に登録されているかをみる。この検索の結果がデータベース 206 から得られて (307)、そのユーザ 211 の認証情報が登録されていれば、その一般ユーザ 211 が認証されたと判定する。

【0017】

尚、ここでは認証機構 A (204) は、チャレンジ・レスポンスを利用した認証を実行することができるが、この認証形態は本発明の趣旨ではないので、ここでは詳しく説明しない。

【0018】

図 4 は、図 3 に示す機能ブロック図における処理の流れを説明するフローチャートで、この処理を実行するプログラムはプログラムメモリ 101 に記憶されており、CPU 100 の制御の下に実行される。

【0019】

データ処理装置が起動されるとまずステップS1で、認証機構切り替え部201に対して、有効な認証機構を問い合わせる。そしてステップS2に進み、有効であると指示された認証機構（ここでは認証機構A（204））を起動する。次にステップS3に進み、ユーザに対してカードリーダー104にカードを挿入するように指示するカード挿入指示画面を表示部103に表示する。

【0020】

次にステップS4に進み、そのユーザのカードがカードリーダー104に挿入されるのを待ち、カードが挿入されるとステップS5に進み、その挿入されたカードの情報を読み取る。そしてステップS6で、その読み取った認証情報を認証機構A（204）に渡す。次にステップS7に進み、認証機構A（204）は、その認証情報を基にして認証機構Aのデータベース206を検索する。そしてステップS8で、そのユーザの認証情報が認証機構A（204）のデータベース206に登録されているかを判定し、そのユーザ211の認証情報がデータベース206に登録されていれば認証成功と判断してステップS9に進み、その一般ユーザ211が認証されたと判定する。一方、ステップS8で、そのユーザの認証情報が認証機構A（204）のデータベース206に登録されていない時は認証失敗と判断してステップS10に進み、そのユーザの認証が得られないと判定する。

【0021】

尚、ここでは認証機構A（204）が選択された場合で説明したが、認証機構B（205）が選択された場合も同様にして実現可能であることはいうまでもない。

【0022】

次に図5の機能ブロック図を参照して、ユーザにより認証機構の切り換えが指示された場合を説明する。

【0023】

図5は、本実施の形態に係るデータ処理装置において、認証機構が起動した後ユーザ（管理者）が認証機構切り替えが許されたカードを挿入する場合を説明する図である。このような認証機構切り替えが許されたカードを持つユーザを管

理者 210 と呼ぶことにする。ここでは、ユーザは予め第一の認証機構にユーザレベルで認証済みであり、カードを用いて、管理者権限の認証レベルを管理する第二の認証機構に認証機構を切り替える実施形態を示す。

【0024】

管理者ユーザ 210 がカードをカードリーダー 104 に挿入すると (500)、カードリーダー制御部 220 は、そのカードに記録された情報を読み取って、認証機構の切り替えが許されたカードであると判断すると、認証機構切り替え部 201 に、そのカードに記録された認証情報を渡す (501)。認証機構切り替え部 201 は、その渡された認証情報を基に、管理者データベース 202 に対して検索をかける (502)。この管理者データベース 202 に、そのカードに記録された情報が登録されている場合に認証が成功したことになる。認証が成功したことが検索結果 (503) に基づいて判定されると、認証機構切り替え部 202 は、認証機構の選択を促す画面を表示するように、ユーザインターフェース制御部 208 に対して要求する (504)。この要求を渡されたユーザインターフェース制御部 208 は、このデータ処理装置に搭載された認証機構の一覧を表示部 103 に表示する。管理者ユーザ 210 が、この表示された一覧に基づいて、所望の認証機構を選択すると (505)、その選択された認証機構名が、ユーザインターフェース制御部 208 から認証機構切り替え部 201 に送られ (506)、有効な認証機構として記憶される。こうして記憶された情報は、次に、このデータ処理装置が起動されたときに認証機構起動部 203 により参照され、これに基づいて認証機構の起動が行われる。

【0025】

図 6 は、図 5 に示す機能ブロック図における処理の流れを説明するフローチャートで、この処理を実行するプログラムはプログラムメモリ 101 に記憶されており、CPU 100 の制御の下に実行される。

【0026】

まずステップ S21 で、カードリーダー 104 にカードが挿入されたかどうかをみる。カードリーダー 104 にカードが挿入されるとステップ S22 に進み、管理者ユーザ 210 が管理者用のカードをカードリーダー 104 に挿入したか、即ち、

認証機構の切り替えが許されたカードが挿入されたかどうかを判断し、そうであればステップS23に進み、認証機構切り替え部201に、そのカードに記録された認証情報を渡して、その管理者が管理者データベース202に登録されている管理者であるかを判定する。そして管理者データベース202に、そのカードに記録された情報が登録されている場合には、認証が成功したとしてステップS24に進み、認証機構の選択を促す認証機構の一覧を表示部103に表示する。次にステップS25に進み、管理者ユーザ210が、この表示された一覧に基づいて、操作パネル105を使用して所望の認証機構を選択すると、その選択された認証機構名が有効な認証機構として記憶される。こうして記憶された情報は、次に、このデータ処理装置が起動されたときに認証機構起動部203により参照され、その認証機構が起動される。この間、ユーザレベルの第一の認証機構においては、ユーザは継続して認証状態であるので、認証が成功し、第二の認証機構名が有効な認証機構として記憶されるのに応答して、第一の認証機構から認証が成功したユーザを管理対象から外すと好適である。切り換え命令に応答してすぐに第一の認証機構からユーザを管理対象外とすると、第二の認証機構で認証が失敗した場合に別の管理者などがいない場合は、課題の欄で述べたように、認証機構や、システム全体を再起動したり、システムを復帰できないことにもなるからである。

【0027】

尚、ステップS22で、プログラムが管理者用のカードが挿入されたのではないと判断した場合、或いはステップS23で、そのカードの持ち主が管理者として登録されていない場合は、その管理者ユーザ210により挿入されたカードは、認証機構の切り替えが許されたカードではないため、何もせずにそのまま処理を終了する。この間、ユーザレベルの認証機構においては、ユーザは継続して認証状態であるので、ユーザレベルの認証機構が管理するシステムに復帰できる。また場合によっては、切り換え前の認証機構の元で動作するシステムにより、「認証の切り換えが失敗した」という旨の表示を操作パネル105に行なってもよい。ここで、第1認証機構の管理下にあるシステムを第1システム、切り換え後の第2認証機構の管理下にあるシステムを第2システムと呼ぶ。

【0028】

このように、カードに記憶されたユーザ名とパスワードの組や、電子証明書などをユーザ認証情報を入力する入力手段の好適な一例であるカードリータ104や操作パネル、カードリーダにおいて入力されたユーザの認証情報を用いて認証切り換え前の第1システムに対する加入権限があるか否かを認証し、認証が成功した場合にはユーザを前記第1システムに加入させる第1認証機構と、入力されたユーザの認証情報を用いて認証切り換え後の第2システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第2システムに加入させる第2認証機構と、前記ユーザを、前記第1システムの管理下で管理するのか、又は、前記第2システムの管理下で管理するのかを制御するプログラムメモリ101に記憶された制御プログラムと、第2認証機構において前記ユーザの前記第2システムに対する認証が成功したことを確認する確認プログラムを説明した。また、第1システムから第2システムの管理下へユーザを移行させる命令を認識した場合には、制御プログラムは、確認プログラムがユーザが第2認証機構にて認証されたことを確認したことを条件として、前記第1システムにおける管理下から前記第2システムにおける管理下に前記ユーザを移行させるべく前記第1認証機構及び前記第2認証機構を制御する。

【0029】

以上説明したように本実施の形態1によれば、複数の認証機構を備える装置において、有効として登録されている認証機構を起動し、その起動された認証機構によりユーザを認証できる。また、その複数の認証機構の中から所望の認証機構を選択してユーザを認証するのに使用できる。

【0030】

[実施の形態2]

本実施の形態2では、複数の認証機構を搭載したデータ処理装置において、ユーザの認証をウェブページと操作パネル105の両方で行う場合で説明する。

【0031】

図7は、本発明の実施の形態2に係るデータ処理装置のハードウェア構成を示すブロック図で、前述の実施の形態1と共通する部分は同じ記号で示し、その説

明を省略する。

【0032】

この実施の形態2に係るデータ処理装置は、通信回線71を介して通信を行うネットワークボード70が設けられている。

【0033】

図8は、本実施の形態2に係るデータ処理装置の機能構成を示す機能ブロック図で、前述の実施の形態1と共通する部分は同じ記号で示している。尚、この実施の形態2においても実施の形態1と同様に、これら各機能部は、CPU100がプログラムを実行することにより実現されている。

【0034】

202は管理者データベースで、管理者の名前などの情報を保存している。認証切り替え部201は、現在有効な認証機構を記憶していて、その有効な認証機構に切り換えることができる。認証機構起動部203は、起動すべき認証機構を判断する機構を持つ。204と205はそれぞれ、このデータ処理装置に搭載されている複数の認証機構の内2つを示し、それぞれ認証機構Aと認証機構Bで示されている。206、207はそれぞれユーザの名前などの情報が保存されている認証機構データベースであり、それぞれ認証機構A(204)用のものと、認証機構B(205)用のものがある。703は液晶パネル制御部で、操作パネル105と表示部103とを制御している。700は認証機構切り替えウェブページ提示部で、認証機構を切り替えるためのウェブページを構築し、管理者210が操作する管理者ウェブブラウザ701にネットワーク経由で表示データを提供する。この認証機構切り替えウェブページ提示部700は、管理者210を認証するためのウェブページも提供している。そのために管理者データベース202をも管理する。702は複数の認証機構で共有する認証機構ウェブページ提示部で、ユーザを認証するためのウェブページを、ユーザ211が操作するブラウザ704にネットワーク経由で提供する。管理者のウェブブラウザ701と、一般ユーザのウェブブラウザ704は、ユーザが操作するコンピュータ上で動作するウェブブラウザであり、言うまでもなくこのデータ処理装置には含まれない。

【0035】

図9は、本実施の形態2に係るデータ処理装置の起動時におけるソフトウェアコンポーネント（図8）間のやりとりを説明する図である。

【0036】

まず、このデータ処理装置の起動時には、認証機構起動部203に制御が渡される。この認証機構起動部203は、無条件に認証機構切り替えウェブページ提示部700を起動する（801）。そして、この認証機構起動部203は、認証機構切り替え部201に有効な認証機構を問い合わせる（802）。その結果により（803）、認証機構A（204）或いは認証機構B（205）を起動する（804）。この図8では、認証機構A（204）が有効であるため、認証機構A（204）を起動する場合を示している。こうして起動された認証機構A（204）は、認証機構ウェブページ提示部702に認証画面を表示するよう要求する（805）。この要求を受けた認証機構ウェブページ提示部702は、ユーザの名前などの認証情報を入力するように促す画面を表示部103に表示する。これに応じて、一般ユーザのウェブブラウザ704を介して、操作パネル105からユーザにより認証情報が入力されると（806、807）、認証機構ウェブページ提示部702は、その入力された認証情報を認証機構A（204）に渡す（808）。これにより認証機構A（204）は、その入力された認証情報を基に認証機構Aの認証機構データベース206に対して検索をかける（809）。この検索の結果（810）に応じて、そのユーザ211が認証されるかどうか決定され、それが認証機構ウェブページ提示部702に通知される（811）。ここで、認証機構A（204）と認証機構ウェブページ提示部702との間でチャレンジ・レスポンスを利用した認証を実行することができるが、この認証形態は本発明の趣旨ではないので、その説明を省略する。

【0037】

図10は、図9に示す機能ブロック図における処理の流れを説明するフローチャートで、この処理を実行するプログラムは図7のプログラムメモリ101に記憶されており、CPU100の制御の下に実行される。

【0038】

この処理はデータ処理装置が起動されることにより開始され、まずステップS

31で、無条件に認証機構切り替えウェブページ提示部700を起動して認証機構切り替えウェブページを表示する。次にステップS32に進み、認証機構切り替え部201に有効な認証機構を問い合わせる。そしてステップS33で、有効な認証機構A(204)或いは認証機構B(205)を起動する。こうして起動された認証機構は、ユーザの名前などの認証情報を入力するように促す画面を表示部103に表示する。次にステップS35に進み、一般ユーザのウェブブラウザ704を介して、ユーザにより操作パネル105から認証情報が入力されるのを待ち、認証情報が入力されると、その入力された認証情報を、有効な認証機構に渡す。これにより、その認証機構は、その入力された認証情報を基に、その認証機構の認証機構データベースに対して検索をかける(ステップS36)。この検索の結果、そのユーザ名等がその認証機構データベースに登録されていればステップS38に進み、そのユーザが認証されたものと判定する。これに対してステップS37で登録されていない場合はステップS39に進み、そのユーザが認証されないと決定する。この結果は認証機構ウェブページ提示部702に通知されて表示される。

【0039】

図11は、本実施の形態2に係るデータ処理装置が起動された後に、管理者ユーザが認証機構切り替える場合を説明する図である。このような権限を持つユーザを管理者と呼ぶ。

【0040】

まず管理者ユーザ210は、管理者ウェブブラウザ701を用いて(901)認証機構切り替えウェブページ提示部700にアクセスする(902)。これにより、管理者ウェブブラウザ701には認証画面が表示される。そこで管理者ユーザ210は、名前などの認証情報を入力する(904, 905)。こうして入力された認証情報は、認証機構切り替えウェブページ提示部700から認証機構切り替えウェブページ提示部700に渡される(910)。この渡された認証情報を基に、認証機構切り替えウェブページ提示部700は管理者データベース202に対して検索をかける(906)。そして管理者データベース202に応答により(907)、その入力された認証情報が登録されている場合に、その管理

者の認証が成功する。こうして認証が成功すると、このデータ処理装置に搭載された認証機構の一覧が掲載されたウェブページを管理者のウェブブラウザ701に提示する(903)。これにより管理者210は、この一覧を参照して、所望の認証機構を選択すると(908)、その選択された認証機構名が認証機構切り替えウェブページ提示部700、認証機構切り替え部201に渡り(909, 910)、有効な認証機構として記憶される。こうして記憶された情報は、次に該装置を起動したときに認証機構起動部203により参照され、その有効として記憶された認証機構が起動される。

【0041】

図12は、図11に示す機能ブロック図における本実施の形態2に係る処理の流れを説明するフローチャートで、この処理を実行するプログラムはプログラムメモリ101に記憶されており、CPU100の制御の下に実行される。

【0042】

まずステップS41で、管理者ユーザ210は、管理者ウェブブラウザ701を用いて認証機構切り替えウェブページ提示部700にアクセスし、管理者ウェブブラウザ701に認証画面を表示する。次にステップS42で、管理者ユーザ210により名前などの認証情報が入力されるとステップS43に進み、入力された認証情報が、管理者データベース202に登録されているか否かを認証機構切り替えウェブページ提示部700により検索し、登録されていればステップS44に進み、このデータ処理装置に搭載された認証機構の一覧が掲載されたウェブページを管理者のウェブブラウザ701に提示する。これにより表示部103にその一覧が表示される。そしてステップS45に進み、管理者210がこの一覧を参照して、所望の認証機構を選択するとステップS46に進み、その選択された認証機構名が認証機構切り替えウェブページ提示部700、認証機構切り替え部201に渡り(909, 910)、有効な認証機構として登録される。こうして記憶された情報は、次に該装置を起動したときに認証機構起動部203により参照され、その有効として記憶された認証機構が起動される。

【0043】

一方、ステップS43で、その入力された認証情報が管理者として登録されて

いない時はステップS47に進み、その管理者の認証情報が登録されていない旨を表示部103に表示する。尚、このステップS47の処理は例えば前述の図6のステップS22、ステップS23で「No」の場合に実行されても良い。

【0044】

以上説明したように本実施の形態2によれば、複数の認証機構を備える装置において、有効として登録されている認証機構を起動し、その起動された認証機構のウェブページにユーザのウェブブラウザによりアクセスしてユーザを認証できる。

【0045】

また、ウェブブラウザにより認証切り替えウェブページにアクセスして、複数の認証機構の中から所望の認証機構を選択してユーザを認証するのに使用できる。

【0046】

[実施の形態3]

次に本発明の実施の形態3に係るデータ処理装置について説明する。

【0047】

図13は、本実施の形態3に係るデータ処理装置の機能構成を示す機能ブロック図で、前述の実施の形態と共通する部分は同じ記号で示している。尚、この実施の形態3に係るデータ処理装置のハードウェア構成は前述の実施の形態1と同様であるため、その説明を省略する。この実施の形態3の特徴は、ユーザの認証をユーザインターフェース制御部208のより制御される操作パネル105からの入力により行うことを特徴としている。

【0048】

認証切り替え部201は、現在有効な認証機構を記憶している。認証機構起動部203は、この認証切り替え部201よりの有効な認証機構を示す情報に基づいて、有効とされている認証機構を起動する。204と205は、このデータ処理装置に搭載されている複数の認証機構の内2つを示し、それぞれ認証機構Aと認証機構Bで示す。206と207は、各認証機構毎にユーザの名前などの情報を保存している認証機構データベースであり、それぞれ認証機構A(204)用

のものと、認証機構B（205）用のものを含む。208は、複数の認証機構で共有するユーザインターフェース制御部で、このデータ処理装置の操作パネル105と表示部103とを制御する。

【0049】

図14は、本実施の形態3に係るデータ処理装置における図13で示したソフトウェアコンポーネント間のやりとりを示した図である。

【0050】

まずこのデータ処理装置の起動時に、認証機構起動部203に制御が渡されると、この認証機構起動部203は、認証機構切り替え部201に有効な認証機構を問い合わせる（1300）。その結果（1301）により、認証機構A（204）又は認証機構B（205）を起動する。この図14では、認証機構A（204）が有効な認証機構として起動される場合を示している。こうして起動された認証機構A（204）は、ユーザインターフェース制御部208に認証画面を表示するよう要求する（1304）。この要求を受けたユーザインターフェース制御部208は、ユーザの名前などの認証情報を入力するように促す画面を表示部103に表示する。この表示に基づいて、ユーザ211により操作パネル105を使用して認証情報が入力されると（1305）、ユーザインターフェース制御部208は、その操作パネル105から入力された認証情報を認証機構A（204）に渡す（1306）。これにより認証機構A（204）は、その認証情報を基に、認証機構Aの認証機構データベース206に対して、ユーザ211の認証情報が登録されているかを調べる（1307）。その結果（1308）に応じて、ユーザ211が認証されるかどうかが決定的にされ、その結果がユーザインターフェース制御部208に送られて表示される（1309）。

【0051】

図15は、図14に示す実施の形態3に係る機能ブロック図における処理の流れを説明するフローチャートで、この処理を実行するプログラムはプログラムメモリ101に記憶されており、CPU100の制御の下に実行される。

【0052】

この処理はデータ処理装置が起動されることにより開始され、まずステップS

51で、有効な認証機構を判定して、有効として記憶されている認証機構A(204)又は認証機構B(205)を起動する。こうして認証機構が起動されるとステップS52に進み、ユーザインターフェース制御部208により認証画面を表示部103に表示する。次にステップS53では、この表示に基づいて、操作パネル105を使用して、ユーザ211により認証情報が入力されるのを待ち、認証情報が入力されるとステップS54に進み、その入力された認証情報を、その認証機構に渡す。これによりステップS55で、その認証機構は、その入力された認証情報を基に、その認証機構の認証機構データベースに、その入力されたユーザ211の認証情報が登録されているか検索する。登録されている時はステップS56に進み、そのユーザ211が認証されたと判定する。一方、ステップS55で登録されていない時はステップS57に進み、そのユーザが認証ができなかったと判断する。

【0053】

図16は、本実施の形態3において、認証機構が起動した後にユーザ(管理者)が認証機構を切り替える場合のソフトウェアコンポーネント間のやりとりを表す図である。このような権限を持つユーザを管理者と呼ぶことにする。

【0054】

管理者ユーザ210が、前述と同様な手順で管理者として認証された後のやりとりを説明する。管理者ユーザ210が管理者として認証された後、管理者ユーザ210は、操作パネル105によりユーザインターフェース制御部208を用いて、適当な方法で認証機構選択画面を表示部103に表示させる。このような機能の実装はメニューシステムなどを使えば自明なので省略する。こうして認証機構の選択画面が表示される。この選択画面には、このデータ処理装置に搭載されている認証機構の一覧が表示される。管理者210は、この表示された一覧に基づいて、操作パネル105から所望の認証機構を選択すると(1500)、ユーザインターフェース制御部208は、管理者210に名前などの認証情報の入力を促す画面を表示する。これにより管理者210が、操作パネル105から認証情報を入力すると(1501)、ユーザインターフェース制御部208は、その選択された認証機構に認証情報の検証を依頼する(1502)。ここでは認証

機構B(205)が選ばれたものとする。認証機構B(205)は、受け取った認証情報を基に、認証機構Bデータベース207に検索をかける(1503)。これにより認証機構Bデータベース207は、その検索結果を認証機構B(205)に返す(1504)。そして、その結果が認証成功を表していた場合、選ばれた認証機構名が認証機構切り替え部201に送られ(1505, 1506)、有効な認証機構として記憶される。こうして記憶された情報は、次にこのデータ処理装置を起動したときに認証機構起動部203で参照される。

【0055】

図17は、本実施の形態3に係るデータ処理装置が起動された後に、管理者ユーザが認証機構を切り替える場合を説明する図である。このような権限を持つユーザを管理者と呼ぶ。

【0056】

この処理は認証機構の切り替えが指示されるとことにより開始され、まずステップS61で、管理者ユーザ210が認証情報を入力すると、前述と同様にして管理者データベース202に、その認証情報が登録されているか否かに応じて、管理者として登録されているか否かを判定する(ステップS62)。管理者として登録されていない時はステップS69に進み、登録された管理者ではないため認証機構の切り替えができない旨を表示してこの処理を終了する。

【0057】

ステップS62で、管理者ユーザ210が管理者として認証されるとステップS63に進み、管理者ユーザ210は、ユーザインターフェース制御部208を用いて、適当な方法で認証機構の選択画面を表示させる。これにより、このデータ処理装置に搭載されている認証機構の一覧が表示される。次にステップS64に進み、管理者210は、この表示された一覧に基づいて、操作パネル105を使用して所望の認証機構が選択されるとステップS65に進み、その選択された認証機構を選択する。次にステップS66に進み、管理者ユーザ210に名前などの認証情報の入力を催促する画面を表示する。これにより管理者210が、その認証情報を操作パネル105により入力するとステップS67に進み、その選択された認証機構に認証情報の検証を依頼する。ここでは、その認証機構は、そ

の受け取った認証情報を基に、認証機構データベースを検索し、そのデータベースにその管理者の認証情報が登録されているかを判別する。その結果、登録されていると判断されるとステップS68に進み、その選ばれた認証機構名を認証機構切り替え部201に送って有効な認証機構として登録する。こうして記憶された情報は、次にこのデータ処理装置を起動したときに認証機構起動部203で参照される。

【0058】

以上説明したように本実施の形態3によれば、複数の認証機構を備える装置において、有効として登録されている認証機構を起動し、操作パネルを使用して入力されたユーザの認証情報に基づいて、その認証機構によりユーザを認証できる。また、管理者は操作パネルを用いて、複数の認証機構の中から所望の認証機構を選択してユーザを認証するのに使用できる。

【0059】

尚、前述したデータ処理装置の具体例としては、複写機としての機能以外に、例えばファクシミリやプリンタ等の機能を備えた多機能複写機が挙げられる。この複写機では、一般ユーザは、その時点で選択されている認証機構（実質的にはソフトウェアで構成され、場合によってはカードリーダ等の特定のハードウェアを使用する）を使用して認証された場合にのみ、その複写機を使用してコピーやファクシミリ送信等を行うことができる。もちろん認証不可能なユーザは、この複写機を使用することができない。

【0060】

又、管理者として登録されているユーザは、必要に応じて認証機構を切り換えることができる。こうして認証機構が切り替えられると、例えばウェブページを使用してユーザの認証が可能になったり、また各ユーザが認証のために入力する情報も変更されることになる。これにより一般のユーザの中でも、この複写機を使用可能なユーザが変更されることになる。またこのような認証機構の切り換えにより、この多機能複写機の、例えば基本設定を変更する権限が与えられているユーザと、それ以外のユーザとの区別を付けることもできる。

【0061】

〔その他の実施の形態〕

なお本発明は、複数の機器(例えばホストコンピュータ、インターフェース機器、リーダ、プリンタなど)から構成されるシステムに適用しても、一つの機器からなる装置(例えば、複写機、ファクシミリ装置など)に適用しても良い。又、例えば、スキャナ機能、プリント機能、コピー機能、ファクシミリ機能、プリンタ機能、ネットワーク機能等の複数の機能のうちの、何れか1つの機能のみを有する単一機能の装置においても本発明は適用可能であるし、上記複数の機能のうちの、例えばコピー機能とプリンタ機能の2つの機能を有するデジタル複合機やコピー／ファクシミリ／プリンタ等の3つの機能或いは3つ以上の機能を有するデジタル複合機等の、上記複数の機能のうちの2つ以上の機能を少なくとも有する複合装置においても本発明は適用可能である。

【0062】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUまたはMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成されることは言うまでもない。

【0063】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0064】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、ROMなどを用いることが出来る。

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOS（オペレーティングシステム）などが実際の処理の一部を行い、その処理によって前述した実施形態の機能が実現さ

れる場合も含まれることは言うまでもない。

【0065】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施の形態の機能が実現される場合も含まれることは言うまでもない。

【0066】

以上説明したように本実施の形態によれば、複数の認証機構を備える装置において、認証機構切り替え時に切り替えようとするユーザの認証を行うことができる。また、並列に構成された認証機構を切り替える場合にも、その切り替えを指示したユーザの認証を行うようにしているので、認証機構を切り替えた後に認証情報データベースが変わってしまったために装置を利用できなくなる状況を防ぐことができる。

【0067】

【発明の効果】

以上説明したように本発明によれば、利便性とセキュリティ上の問題を解決することができる。

【0068】

また本発明によれば、認証機構を切り替えた後にユーザが適切な認証情報を持ち合わせていないがために装置を使用することができなくなることを避けるために、認証機構の切り替え前に新しい認証機構によって認証を確認することができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態に係るデータ処理装置のハードウェア構成を説明するブロック図である。

【図2】

実施の形態 1 に係るデータ処理装置の機能構成を説明する機能ブロック図である。

【図 3】

実施の形態 1 に係るデータ処理装置において、カードによりユーザの認証を行う場合を説明する機能ブロック図である。

【図 4】

実施の形態 1 に係るデータ処理装置において、カードによりユーザの認証を行う場合の処理を説明するフローチャートである。

【図 5】

実施の形態 1 に係るデータ処理装置において、管理者により認証機構を切り換える場合を説明する機能ブロック図である。

【図 6】

実施の形態 1 に係るデータ処理装置において、管理者により認証機構を切り換える場合の処理を説明するフローチャートである。

【図 7】

本発明の実施の形態 2 に係るデータ処理装置のハードウェア構成を説明するブロック図である。

【図 8】

実施の形態 2 に係るデータ処理装置の機能構成を説明する機能ブロック図である。

【図 9】

実施の形態 2 に係るデータ処理装置において、ユーザのウェブブラウザを用いてユーザの認証を行う場合を説明する機能ブロック図である。

【図 10】

実施の形態 2 に係るデータ処理装置において、ユーザのウェブブラウザを用いてユーザの認証を行う処理を説明するフローチャートである。

【図 11】

実施の形態 2 に係るデータ処理装置において、管理者のウェブブラウザを用いて認証機構の切り替えを行う場合を説明する機能ブロック図である。

【図 12】

実施の形態 2 に係るデータ処理装置において、管理者のウェブブラウザを用いて認証機構の切り替えを行う処理を説明するフローチャートである。

【図 13】

本発明の実施の形態 3 に係るデータ処理装置の機能構成を説明する機能ブロック図である。

【図 14】

本実施の形態 3 に係るデータ処理装置において、ユーザインターフェースを用いてユーザの認証を行う場合を説明する機能ブロック図である。

【図 15】

本実施の形態 3 に係るデータ処理装置において、ユーザインターフェースを用いてユーザの認証を行う処理を説明するフローチャートである。

【図 16】

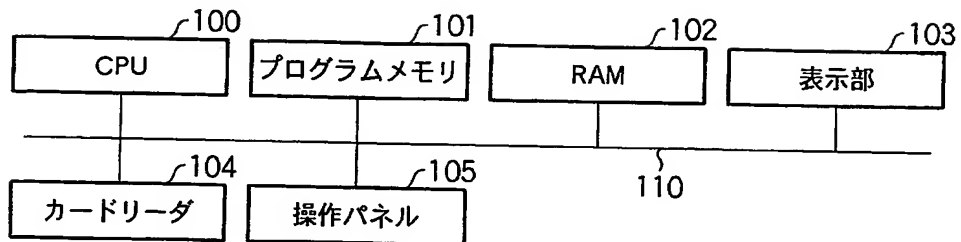
実施の形態 3 に係るデータ処理装置において、管理者がユーザインターフェースを用いて認証機構の切り替えを行う場合を説明する機能ブロック図である。

【図 17】

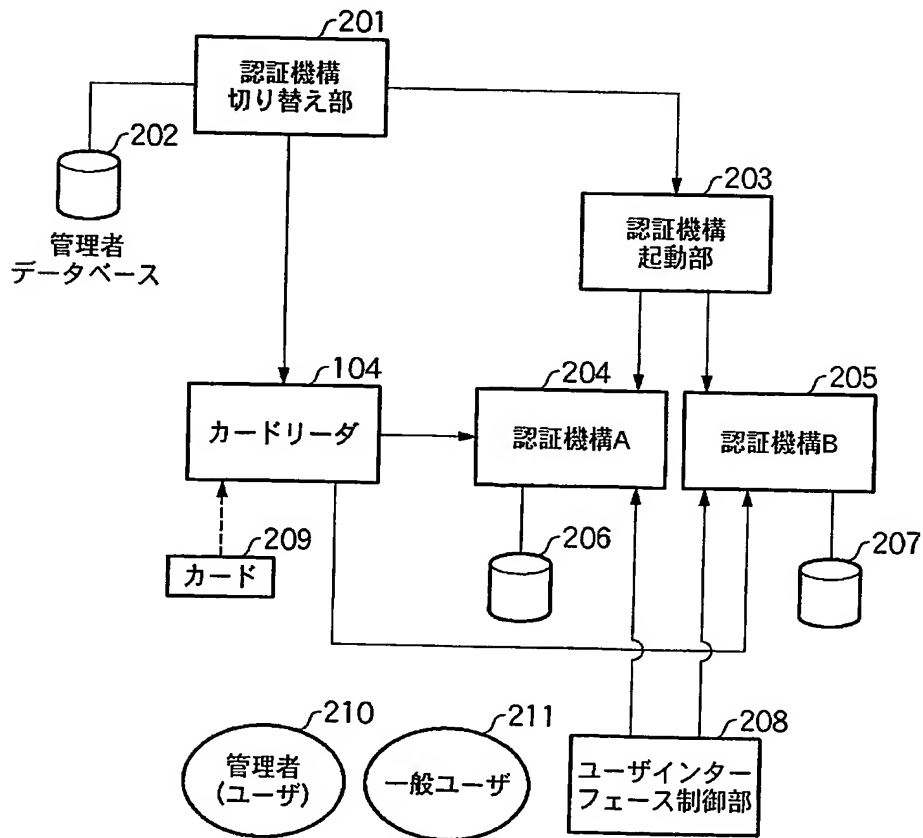
実施の形態 3 に係るデータ処理装置において、管理者がユーザインターフェースを用いて認証機構の切り替えを行う処理を説明するフローチャートである。

【書類名】 図面

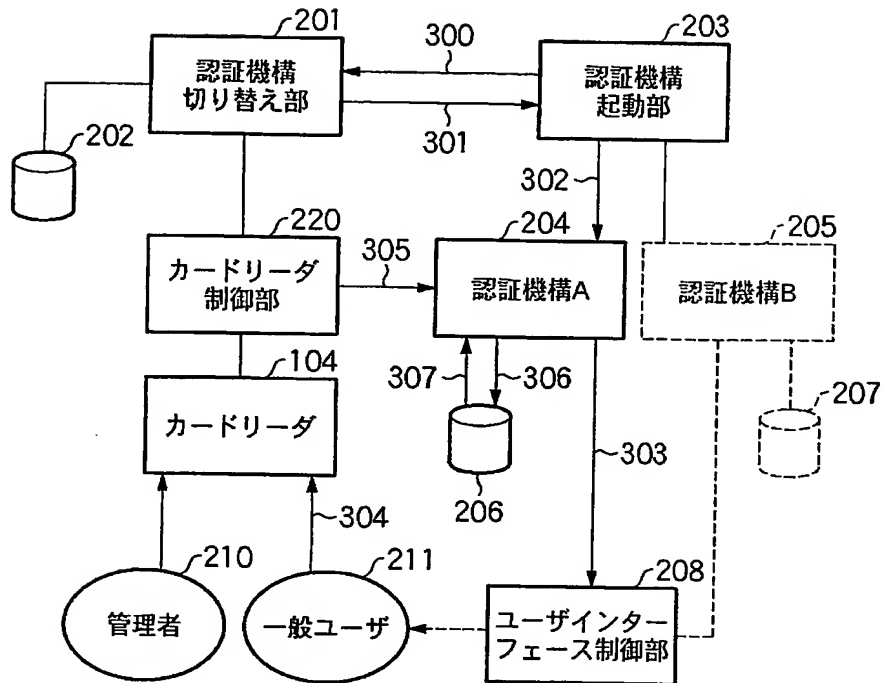
【図 1】



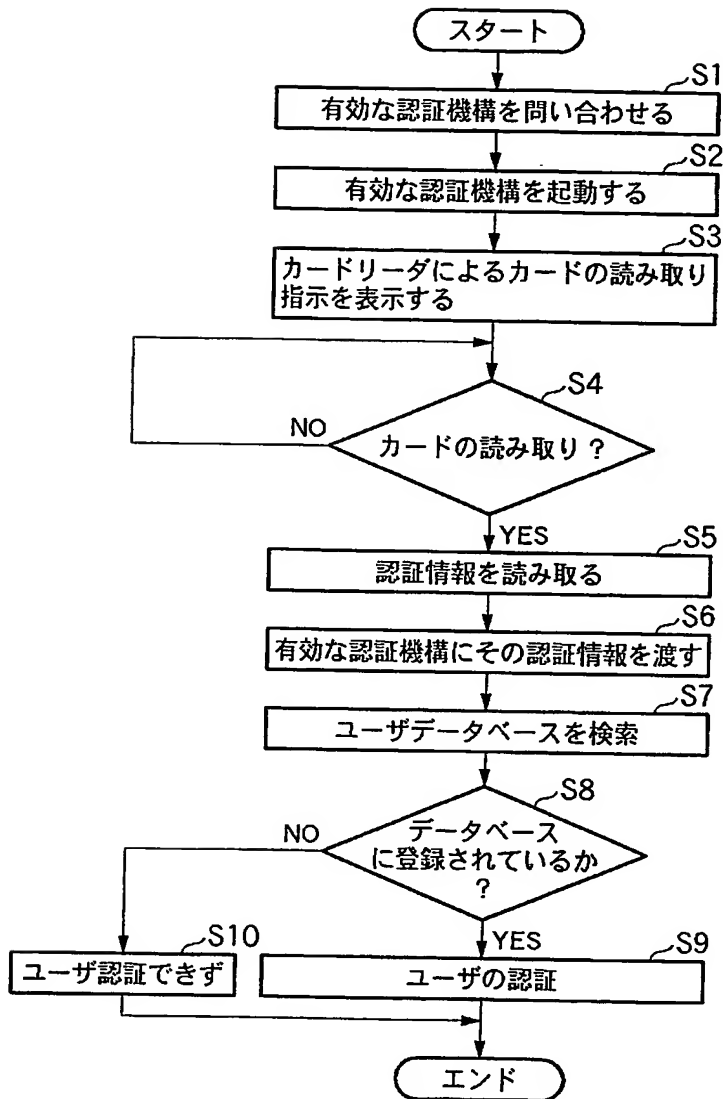
【図 2】



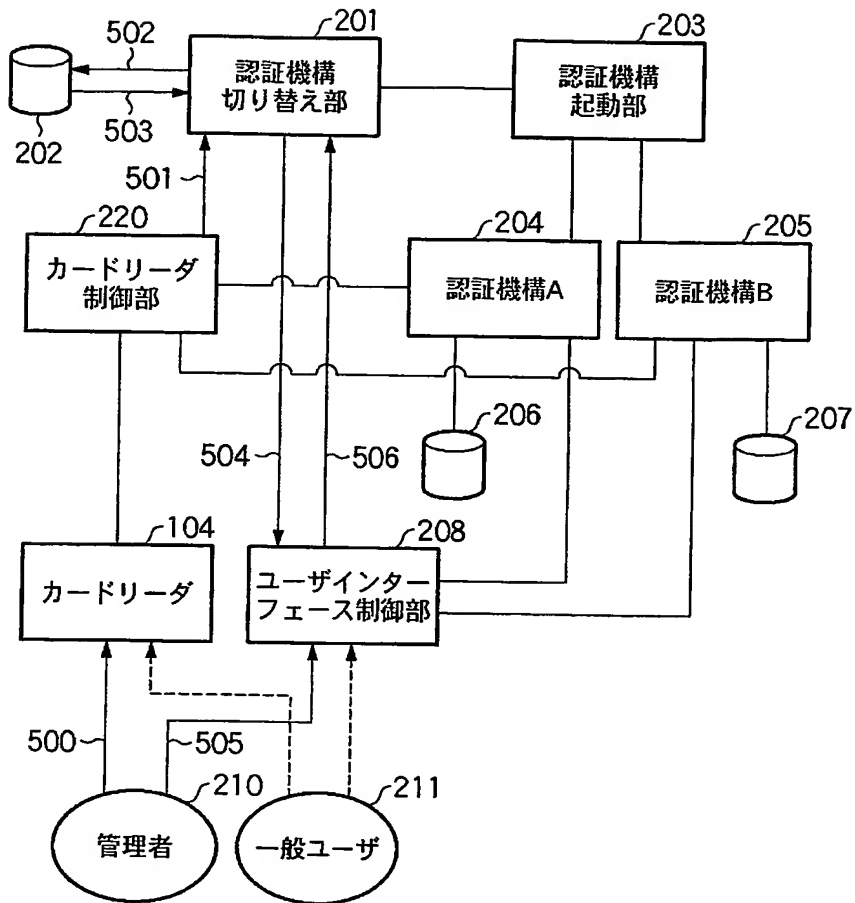
【図 3】



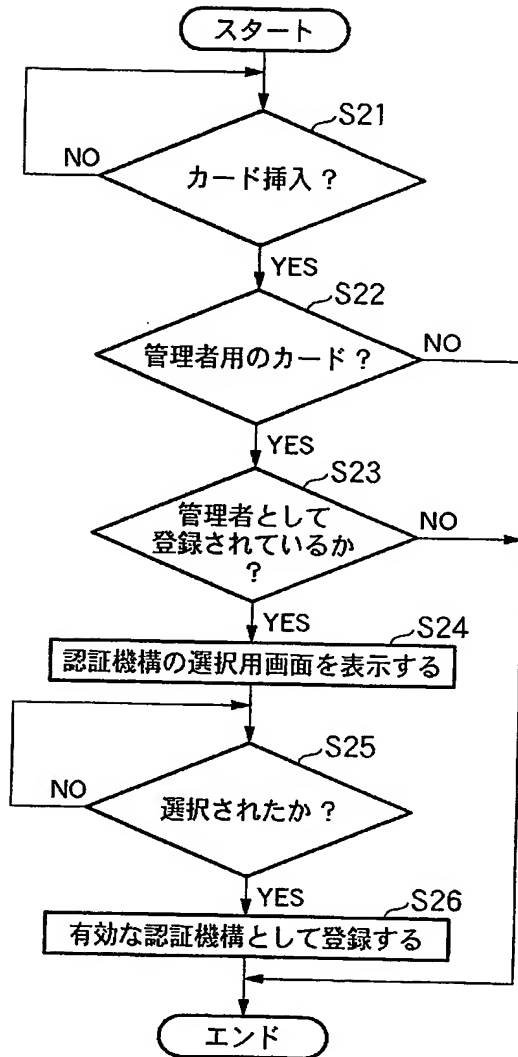
【図 4】



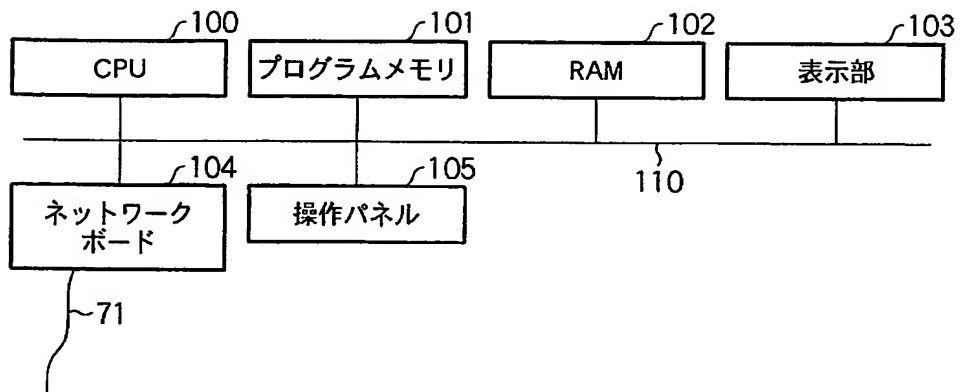
【図 5】



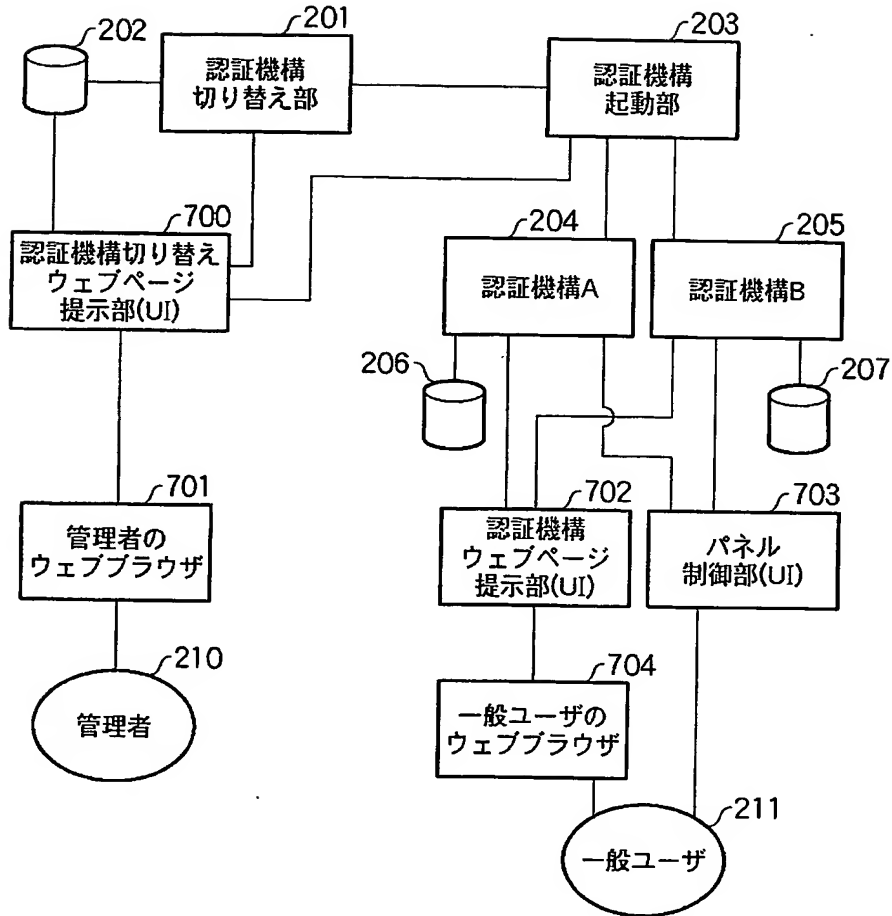
【図 6】



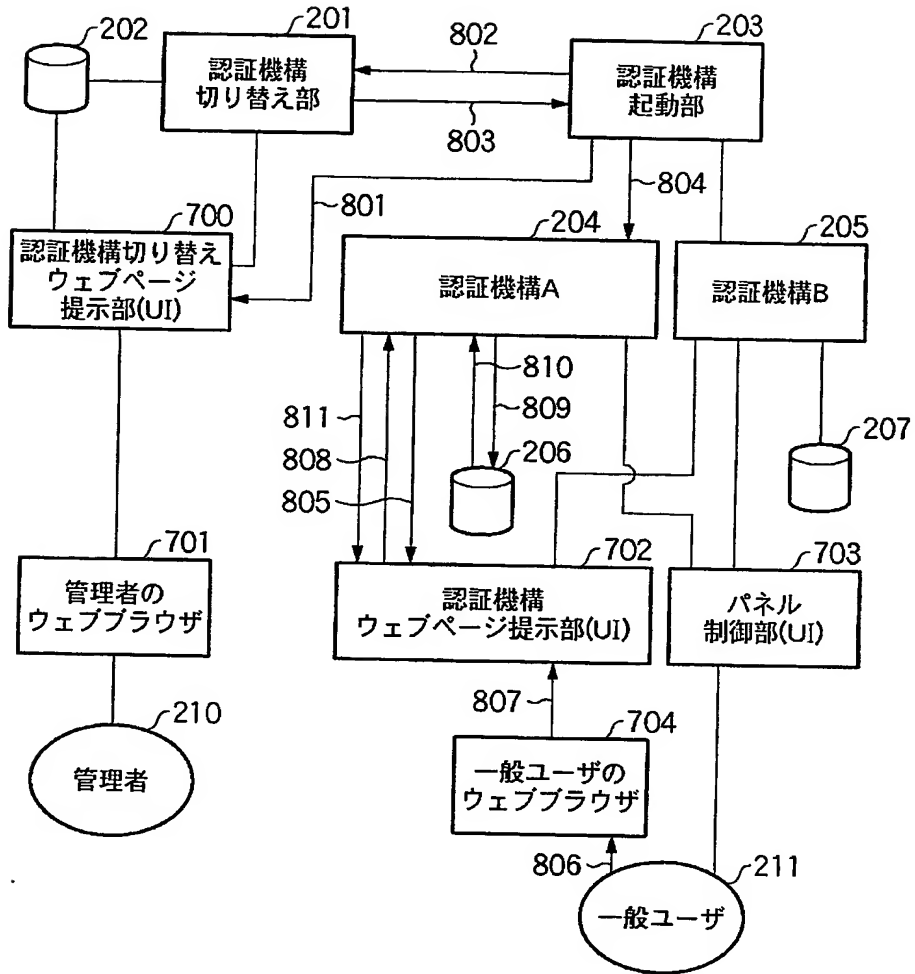
【図 7】



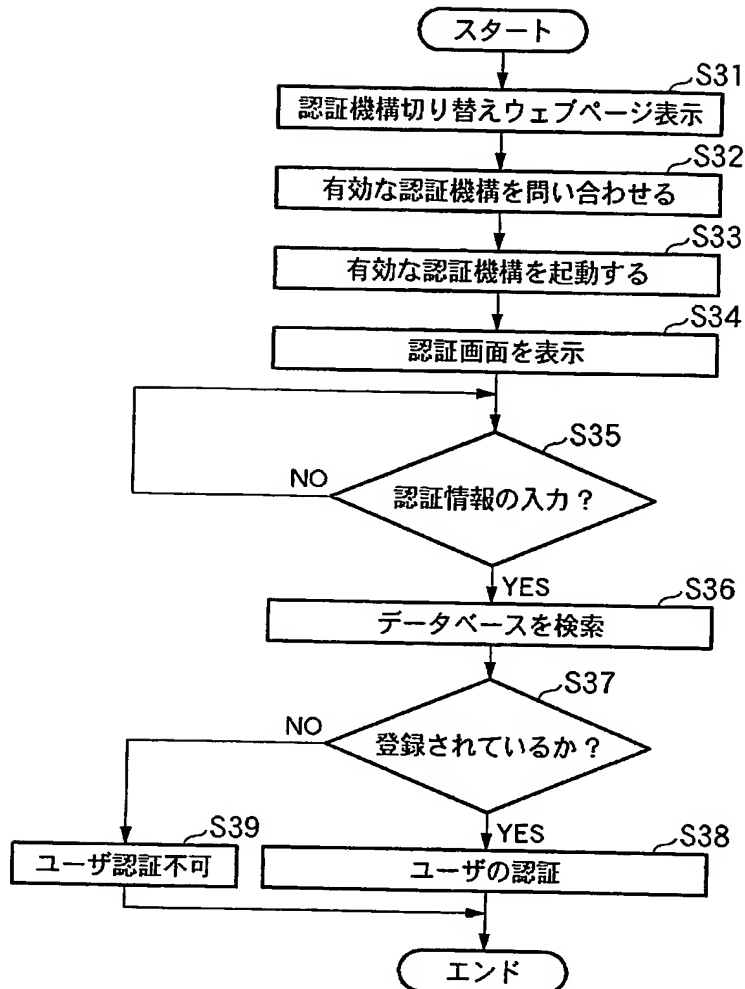
【図 8】



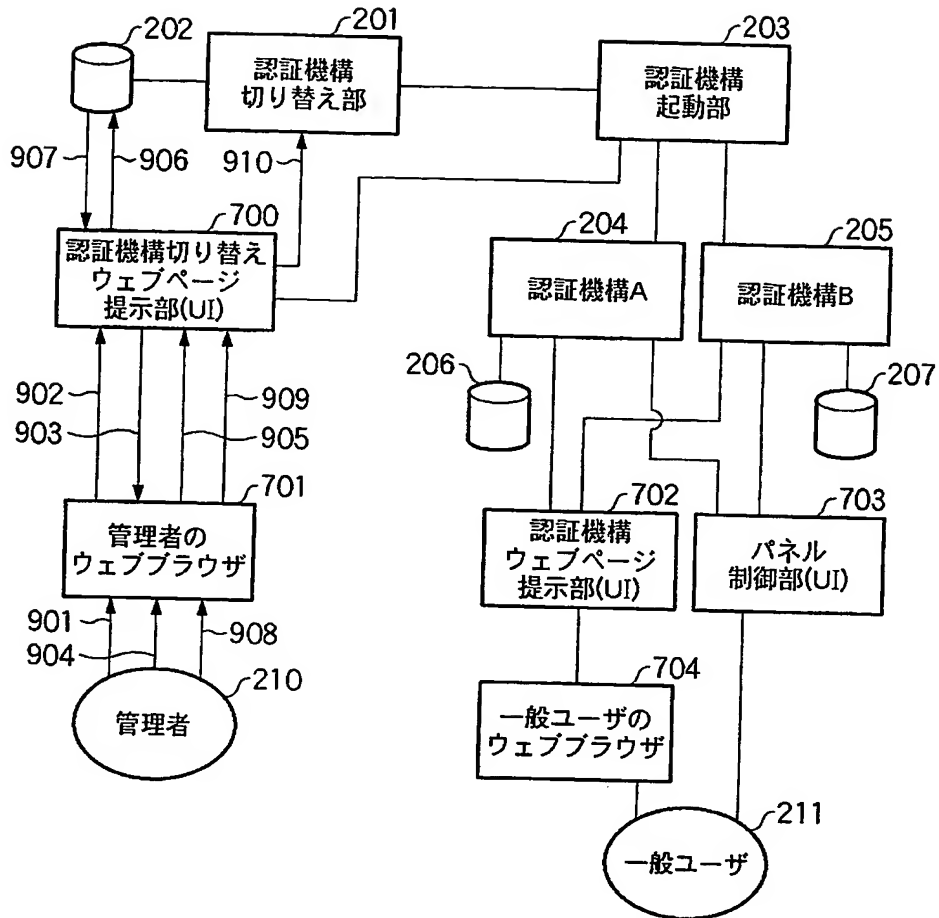
【図 9】



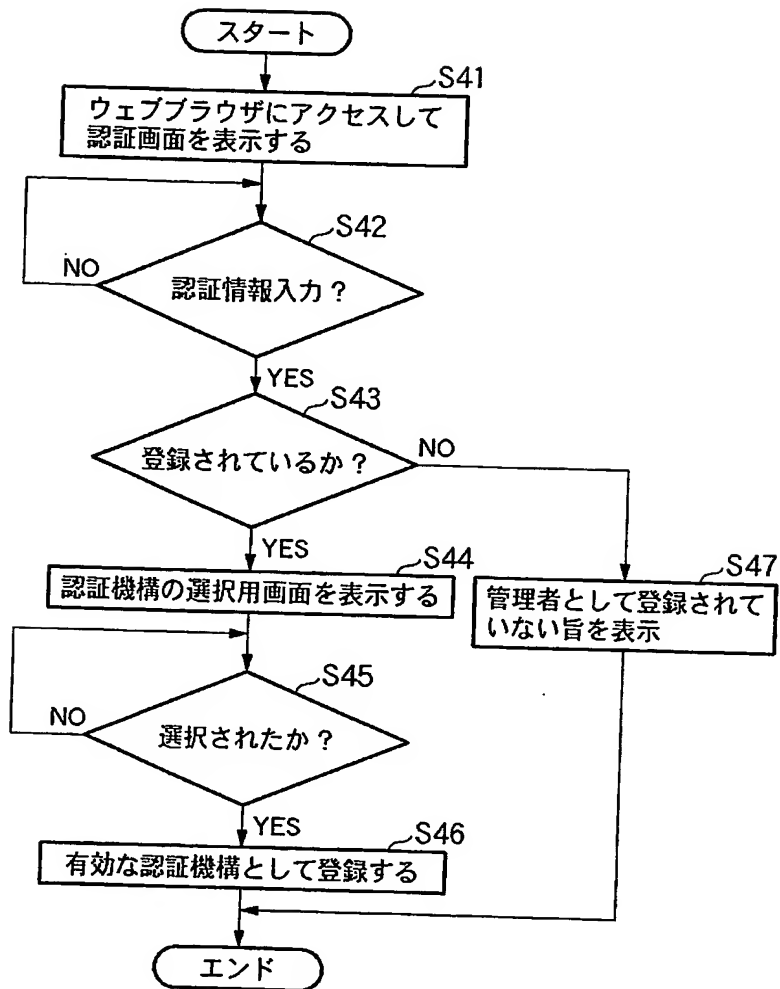
【図10】



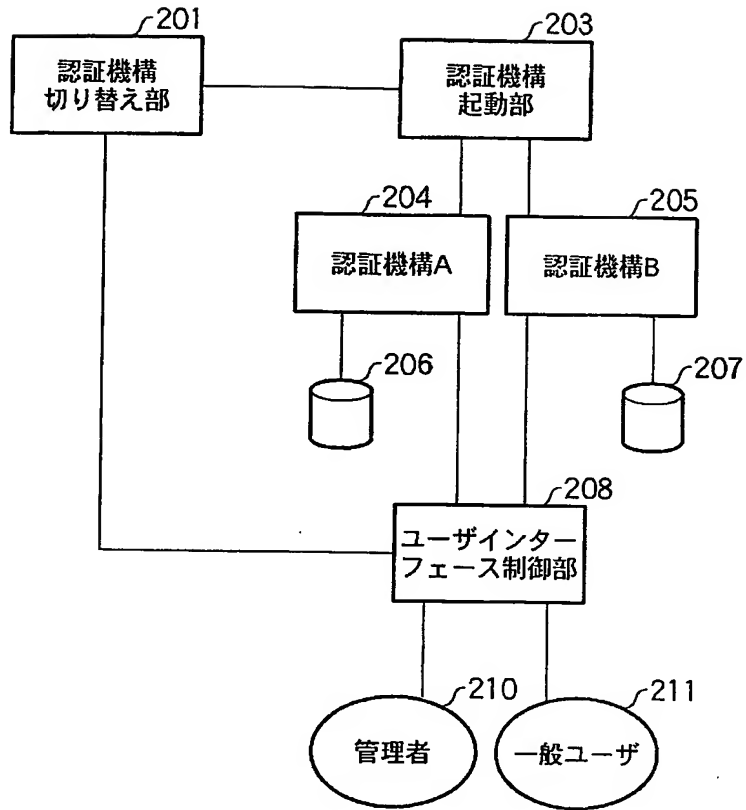
【図 11】



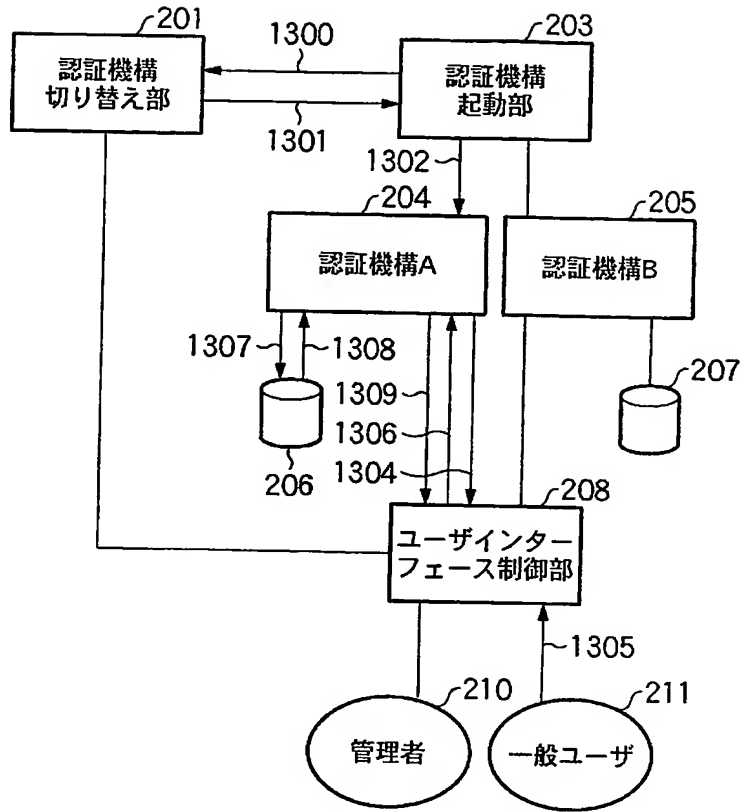
【図 12】



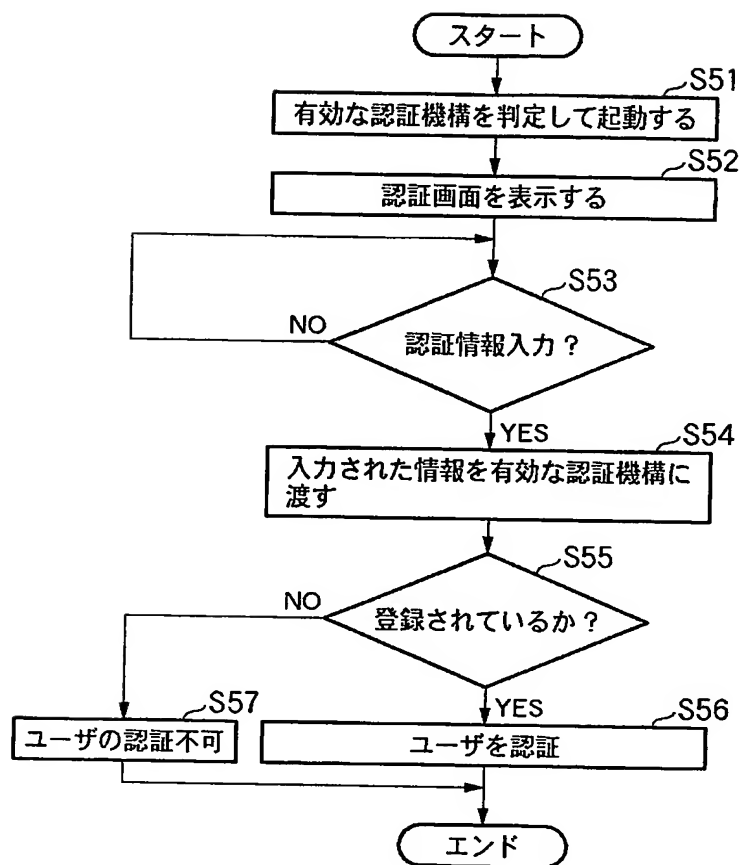
【図 13】



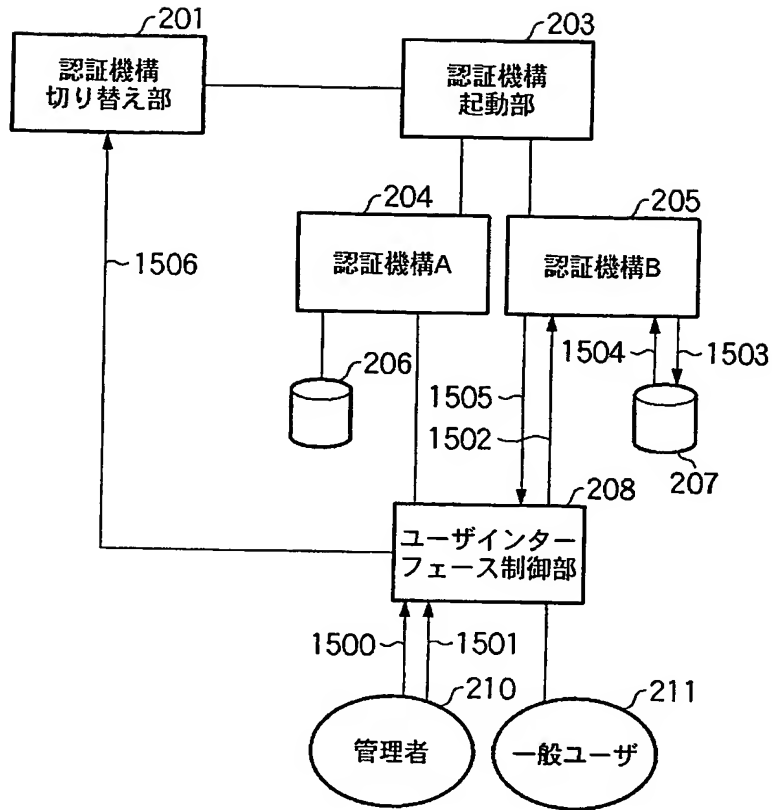
【図 14】



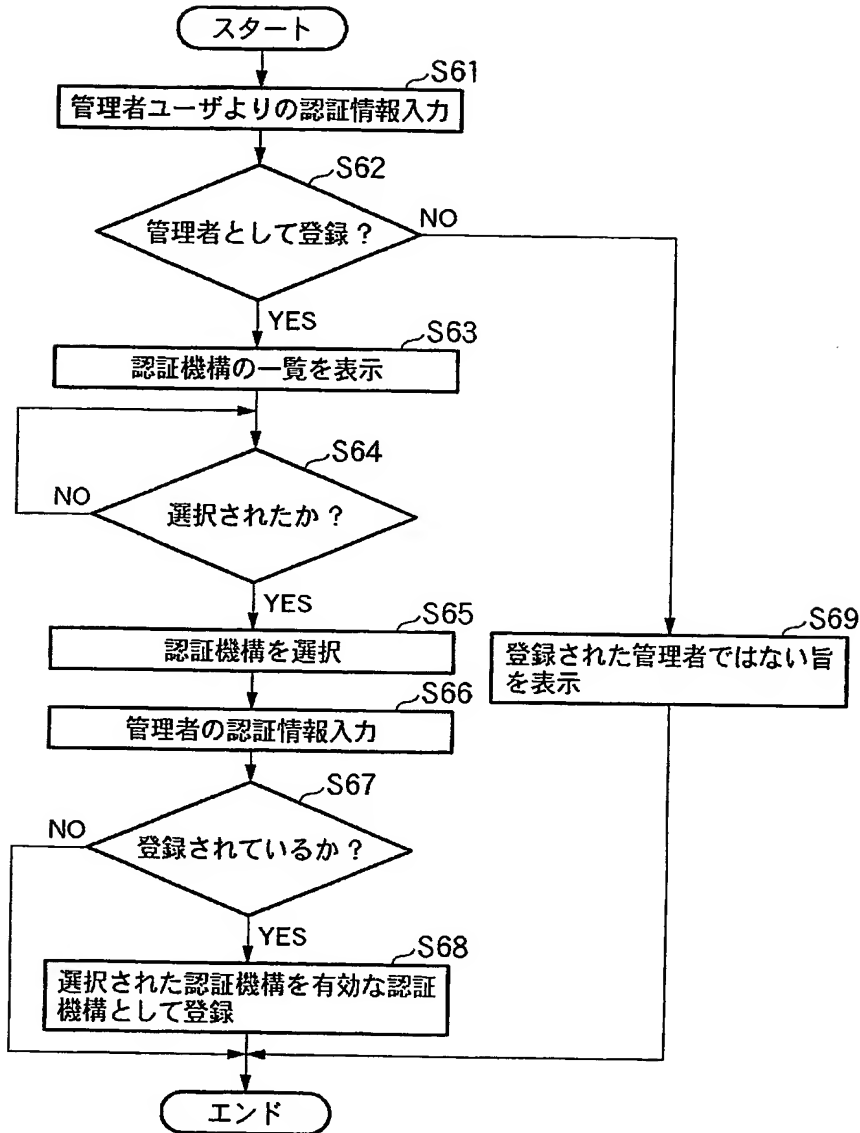
【図 15】



【図16】



【図 17】



【書類名】 要約書

【要約】

【課題】 利便性とセキュリティ上の問題を解決する。

【解決手段】 複数の認証機構を備える認証装置であって、ユーザの認証情報を入力するカードリーダーにより入力された認証情報が複数の認証機構を切換え可能なユーザのものかどうかを判定し（S 2 3）、切換え可能なユーザのものと判定されると複数の認証機構の一覧を表示し（2 4）、その表示された一覧の中の選択された認証機構を有効な認証機構として登録する（S 2 6）。

【選択図】 図 6

特願2003-021039

出願人履歴情報

識別番号

[000001007]

1. 変更年月日
[変更理由]

1990年 8月30日

新規登録

住所
氏名

東京都大田区下丸子3丁目30番2号
キャノン株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.